

Android端末 無線LAN 設定方法

本資料について

- 本資料は、Android端末 が CONTEC製アクセスポイント と無線LAN通信する為の設定方法を記載しています。
- 本資料に記載している内容は、全ての環境での動作を保証するものではありません。
- 本資料の内容は、当社が独自に調査・製作したものであり、Apple.Inc、サムスン電子株式会社、Sony Ericsson Mobile Communications AB、シャープ株式会社、任天堂株式会社、および株式会社ソニー・コンピュータエンタテインメントが認定・承認したものではありません。本資料の内容に関する各社へのお問合せはご遠慮ください。

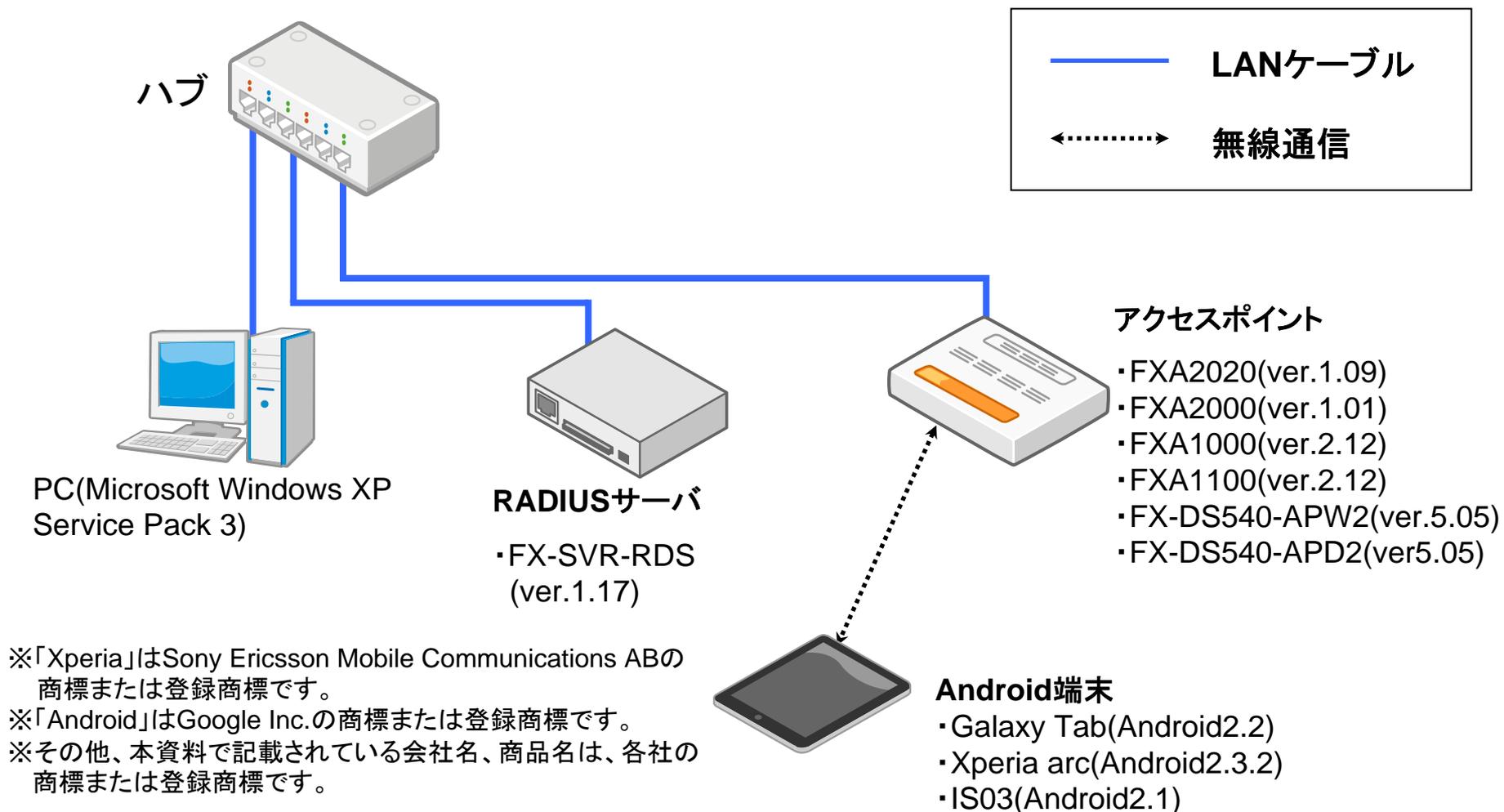
目次

1. 通信環境について
2. WEP・WPA/WPA2-PSKの設定方法
3. EAP-TLSの設定方法
4. PEAPの設定方法
5. 証明書が必要とする場合のPEAPの設定方法

1. 通信環境について

【構成図】

以下の機器構成となります。



2. WEP・WPA/WPA2-PSKの設定方法

【設定方法】

- ①「無線とネットワーク」をタップします。
- ②「Wi-Fi設定」をタップします。



【設定方法】

③「Wi-Fi」をタップしてWi-Fi機能をONにします。

④「Wi-Fiネットワーク」一覧の一番下にある項目「Wi-Fiネットワークを追加」をタップします。



【設定方法】

⑤「ネットワークSSID」にESSIDを入力します。

⑥「セキュリティ設定」をタップして、暗号方式を選択します。

※ESSID,暗号方式,暗号キーはそれぞれのネットワークにより異なります。ご使用の環境に合わせて設定してください。



【設定方法】

⑦「パスワード」に暗号キーを入力して、「保存」をタップします。

⑧右図のように「接続しました」と表示が出れば接続成功です。



3. EAP-TLSの設定方法

【EAP-TLSの設定方法】

EAP-TLS認証を行う場合、RADIUSサーバの設定を行い、クライアント証明書をダウンロード後、証明書をAndroid端末へインストールする必要があります。

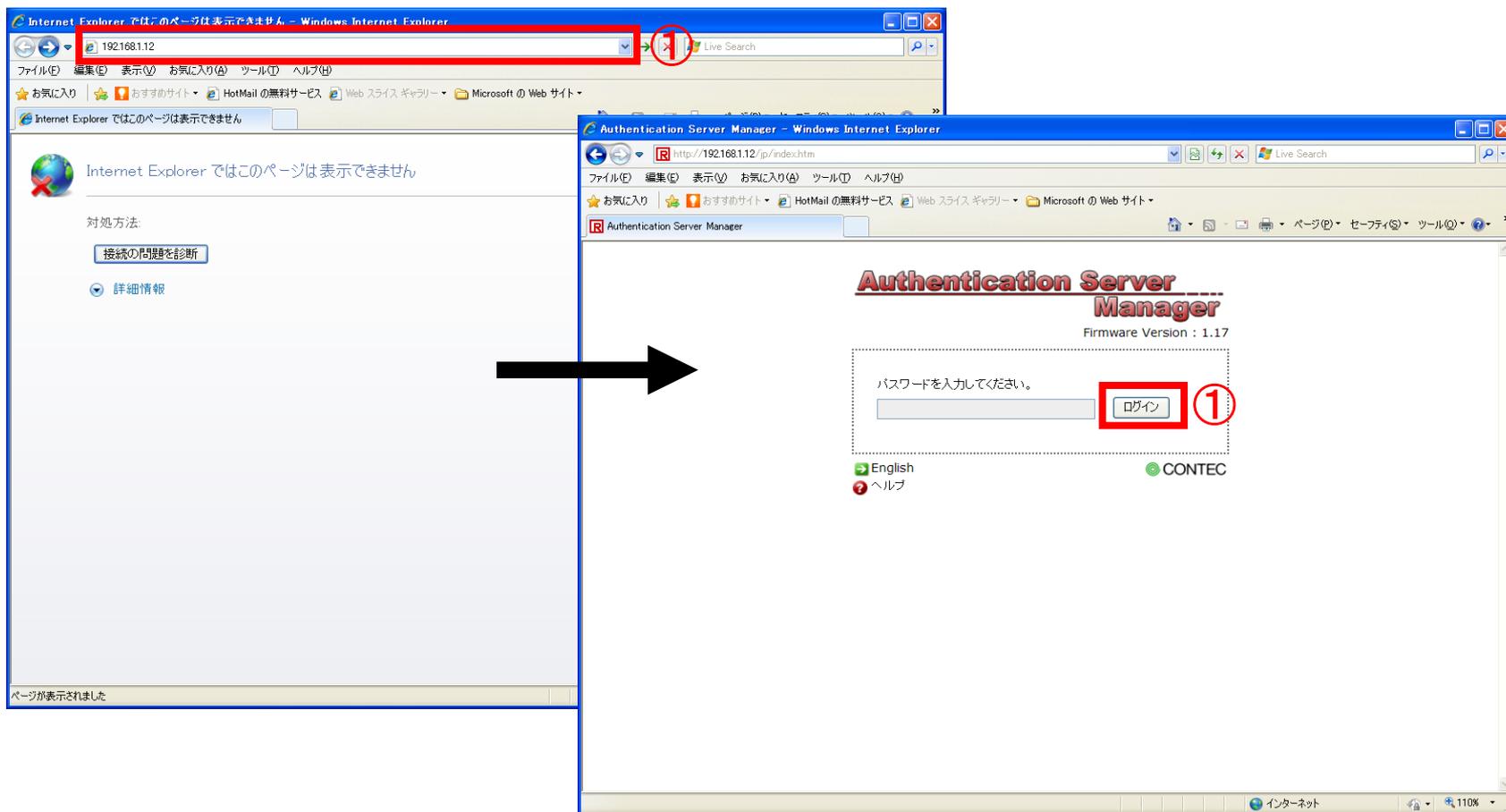
下記 STEP1～3 の手順で設定方法を説明します。

- ・STEP1.RADIUSサーバでクライアント証明書を作成
- ・STEP2.クライアント証明書を端末にインストール
- ・STEP3.ネットワーク設定

【EAP-TLSの設定方法】

STEP1. クライアント証明書を作成します。

①ブラウザのアドレスバーにFX-SVR-RDSのIPアドレスを入力して、機器にログインします。



【EAP-TLSの設定方法】

STEP1. クライアント証明書を作成します。

②「トップ」→「設定」→「基本設定」の順にクリックします。

③基本設定画面で、各項目を入力して、「確定」をクリックします。

The screenshot shows the 'Authentication Server Manager' web interface in Internet Explorer. The browser address bar shows 'http://192.168.1.12/jp/top.htm'. The page title is 'Authentication Server Manager'. The main content area is titled '設定' (Settings) and '基本設定' (Basic Settings). The left sidebar contains a navigation menu with items like 'トップ' (Home), '設定' (Settings), '基本設定' (Basic Settings), '認証局' (Certificate Authority), 'DHCP', 'NTP', 'SNMP', 'ログ機能' (Logging), 'Eメール通知' (Email Notification), '設定一覧' (Settings List), 'ステータス' (Status), 'メンテナンス' (Maintenance), 'English', and 'ヘルプ' (Help). The '基本設定' page contains a form with the following fields:

ホスト名(必須)	host
言語設定	日本語
パスワード
パスワード(確認用)
IPアドレス	192 .168 .1 .12
サブネットマスク	255 .255 .255 .0
デフォルトゲートウェイ	0 .0 .0 .0
DNSサーバ	0 .0 .0 .0
VLAN	VLAN 機能: 無効
	VLAN ID: 0
	設定ファイル暗号化: 無効

At the bottom of the form, there are two buttons: '確定' (Confirm) and 'リセット' (Reset). The '確定' button is highlighted with a red box and the number 3. The navigation menu items 'トップ', '設定', and '基本設定' are also highlighted with a red box and the number 2.

【EAP-TLSの設定方法】

STEP1. クライアント証明書を作成します。

④「認証局」→「認証局情報」の順にクリックします。

⑤認証局情報画面で、
各項目を入力して、「作成」
をクリックします。

④

⑤

⑤

「有効期限」は、デフォルトで「730(日)」と入力されていますが、
変更することも可能です。

【EAP-TLSの設定方法】

STEP1. クライアント証明書を作成します。

⑥「オーセンティケータ」をクリックします。

⑦オーセンティケータ画面

で、各項目を入力して、

「追加」をクリックします。

Authentication Server Manager - Windows Internet Explorer
http://192.168.1.12/ip/top.htm

Authentication Server Manager

CONTEC ver. 1.17

FX-SVR-RDS Authentication Server Manager

設定

オーセンティケータ

オーセンティケータの追加

IPアドレス: 192.168.1.11

共有シークレット: concet_test

追加 クリア

「IPアドレス」には、アクセスポイントのIPアドレスを入力します。
「共有シークレット」には、アクセスポイント側でも同じ値を入力します。

【EAP-TLSの設定方法】

STEP1. クライアント証明書を作成します。

⑧オーセンティケータ一覧に前ページで設定したIPアドレスが追加されている事を確認します。

The screenshot shows the 'Authentication Server Manager' web interface in Internet Explorer. The main content area is titled '設定' (Settings) and 'オーセンティケータ' (Authenticators). Below the 'オーセンティケータの追加' (Add Authenticator) section, there is a table titled 'オーセンティケータ一覧' (Authenticators List). This table is highlighted with a red box and a circled '8' next to it. The table contains one entry with the IP address 192.168.1.11.

No.	IP アドレス	削除 ALL
1	192.168.1.11	<input type="checkbox"/>

Buttons for '削除' (Delete) and 'クリア' (Clear) are located below the table.

【EAP-TLSの設定方法】

STEP1. クライアント証明書を作成します。

⑨「ユーザ管理」をクリックします。

⑩「認証方式」で「EAP-TLS」を選択して、「確定」をクリックします。

The screenshot shows the Authentication Server Manager web interface. The browser address bar displays `http://192.168.1.12/jp/top.htm`. The page title is "Authentication Server Manager ver. 1.17". The main content area is titled "設定" (Settings) and "ユーザ管理" (User Management). The "認証方式" (Authentication Method) is set to "EAP-TLS". The "サーバ証明書" (Server Certificate) section shows the validity period as "2013.07.24 04:03 GMT" and the download options as "DER 形式" and "PEM 形式". The "確定" (Confirm) button is highlighted with a red box and a circled "10".

認証方式	
サーバ証明書	有効期限(日) 2013.07.24 04:03 GMT
	ダウンロード DER 形式 PEM 形式

ユーザ管理	
アカウント	<input type="text"/>
パスワード	<input type="password"/>
パスワード(確認用)	<input type="password"/>

【EAP-TLSの設定方法】

STEP1. クライアント証明書を作成します。

⑪「ユーザ管理」で「アカウント」と「パスワード」を入力して、「追加」をクリックします。

Authentication Server Manager - Windows Internet Explorer

http://192.168.1.12/jp/top.htm

CONTEC ver. 1.17

FX-SVR-RDS Authentication Server Manager

設定

ユーザ管理

認証方式

認証方式	EAP-TLS
サーバ証明書	有効期限(日) 2013.07.24 04:03 GMT
	ダウンロード DER 形式 PEM 形式

確定 クリア

ユーザ管理

新規追加

アカウント	cortec_user
パスワード
パスワード(確認用)

⑪

⑪

追加 クリア

「アカウント」と「パスワード」は、端末でネットワーク接続の設定をする際、入力を求められます。

保存 / 再起動
再起動
保存
ログアウト

インターネット 110%

【EAP-TLSの設定方法】

STEP1. クライアント証明書を作成します。

⑫前ページで追加したアカウントが、「アカウント一覧」に追加されている事を確認して、「発行/変更」をクリックします。

The screenshot shows the Authentication Server Manager web interface. The left sidebar contains a navigation menu with options like '設定' (Settings), 'ステータス' (Status), and 'ヘルプ' (Help). The main content area is divided into sections: 'サーバ証明書' (Server Certificate), 'ユーザ管理' (User Management), and 'アカウント一覧' (Account List). The 'アカウント一覧' section is highlighted with a red box, and the '発行/変更' button for the first account is also highlighted with a red box and a circled '12'.

サーバ証明書

認証方式	EAP-TLS	
サーバ証明書	有効期限(日)	2013.07.24 04:03 GMT
	ダウンロード	DER 形式 PEM 形式

確認 クリア

ユーザ管理

新規追加

アカウント	<input type="text"/>
パスワード	<input type="password"/>
パスワード(確認用)	<input type="password"/>

追加 クリア

アカウント一覧 最新の状態に更新 削除アカウント一覧

No.	アカウント	フィルタ ID	ステータス / 有効期限	クライアント証明書 / 設定変更	削除
1	contec_user		未発行	発行/変更	ALL

アカウント削除 クリア

【EAP-TLSの設定方法】

STEP1. クライアント証明書を作成します。

⑬左下のウィンドウで、「有効期限(日)」を入力して「設定変更」をクリックします。

⑭「PKCS#12(ルート証明書含む)」を選択して、「発行」をクリックします。

デフォルトで「365」と入力されていますが、有効期限を変更することができます。

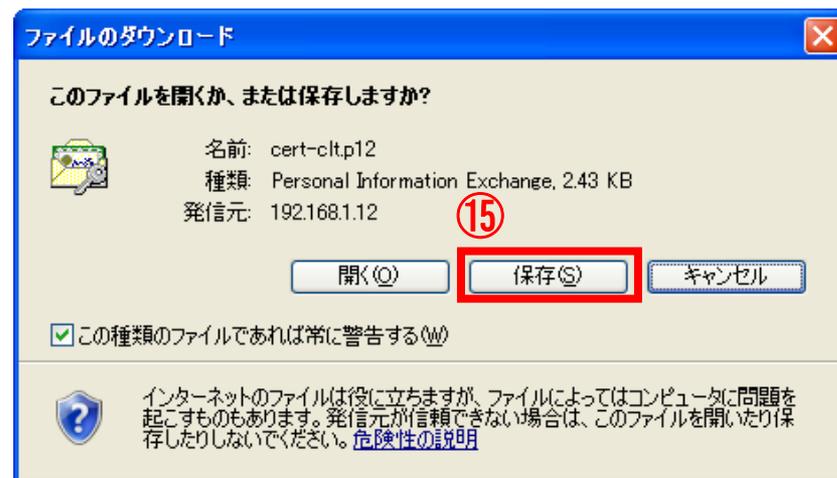
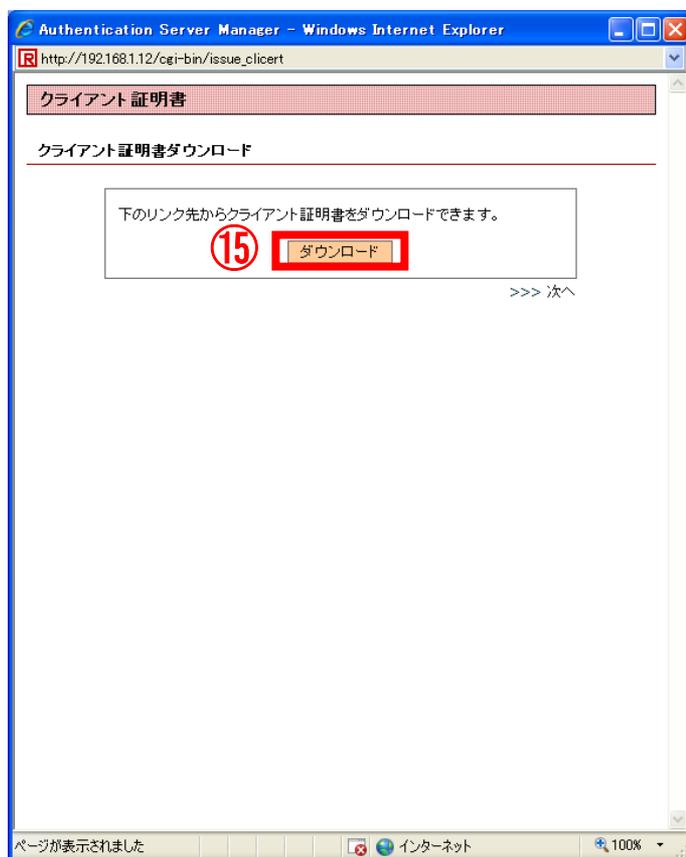
⑬

⑭ PKCS#12 形式(ルート証明書含む) PKCS#12 形式(ルート証明書含まない)
 DER 形式(秘密鍵暗号化有) DER 形式(秘密鍵暗号化無)
 PEM 形式(秘密鍵暗号化有) PEM 形式(秘密鍵暗号化無)

【EAP-TLSの設定方法】

STEP1. クライアント証明書を作成します。

⑮ 「ダウンロード」をクリック後、「保存」で、クライアント証明書をダウンロードします。



【EAP-TLSの設定方法】

STEP1. クライアント証明書を作成します。

⑯「ステータス」に有効期限が記載されている事を確認します。

⑰「保存/再起動」をクリックして、再起動します。

The screenshot shows the Authentication Server Manager web interface. The left sidebar contains a navigation menu with items like '設定' (Settings), 'ステータス' (Status), and '再起動' (Restart). The main content area is divided into sections: '認証方式' (Authentication Method) set to 'EAP-TLS', 'サーバ証明書' (Server Certificate) with expiration date '2013.07.24 04:03 GMT', and 'ユーザ管理' (User Management). Under 'ユーザ管理', there is a '新規追加' (New Addition) form with fields for 'アカウント' (Account), 'パスワード' (Password), and 'パスワード(確認用)' (Password for confirmation). Below that is an 'アカウント一覧' (Account List) table. The table has columns for 'No.', 'アカウント' (Account), 'フィルタID' (Filter ID), 'ステータス / 有効期限' (Status / Validity Period), 'クライアント証明書 / 設定変更' (Client Certificate / Settings Change), and '削除' (Delete). The first row shows account 'contec_user' with status 'ステータス / 有効期限' and expiration date '2012.07.24 04:08 GMT'. A red box highlights the 'ステータス / 有効期限' cell, with a circled '16' next to it. Another red box highlights the '保存 / 再起動' button in the sidebar, with a circled '17' next to it.

No.	アカウント	フィルタID	ステータス / 有効期限	クライアント証明書 / 設定変更	削除
1	contec_user		ステータス / 有効期限 2012.07.24 04:08 GMT	発行/変更	ALL

以上で、クライアント証明書の作成は完了です。

【EAP-TLSの設定方法】

STEP2. クライアント証明書を端末にインストールします。

端末にクライアント証明書をインストールするには、microSDカードが必要です。microSDカードにSTEP1.⑮でダウンロードしたクライアント証明書を保存して、端末に挿入してください。

【EAP-TLSの設定方法】

STEP2. クライアント証明書を端末にインストールします。

①「位置情報とセキュリティ」をタップします。

②「証明書のインストール」をタップします。

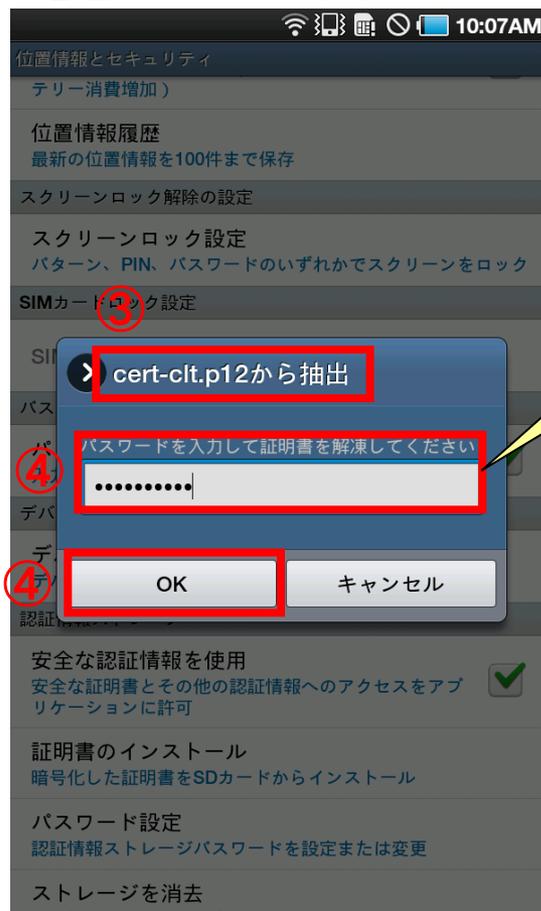


【EAP-TLSの設定方法】

STEP2. クライアント証明書を端末にインストールします。

③SDカード内にあるクライアント証明書ファイル名が表示されます。

④パスワードを入力して、「OK」をタップします。



STEP1.⑪で設定した
パスワードを入力

【EAP-TLSの設定方法】

STEP2. クライアント証明書を端末にインストールします。

⑤証明書名のウィンドウが表示されます。既に証明書名が入力されているので、そのまま「OK」をタップしても問題ありませんが、ここでは「contec_wlan」として設定します。

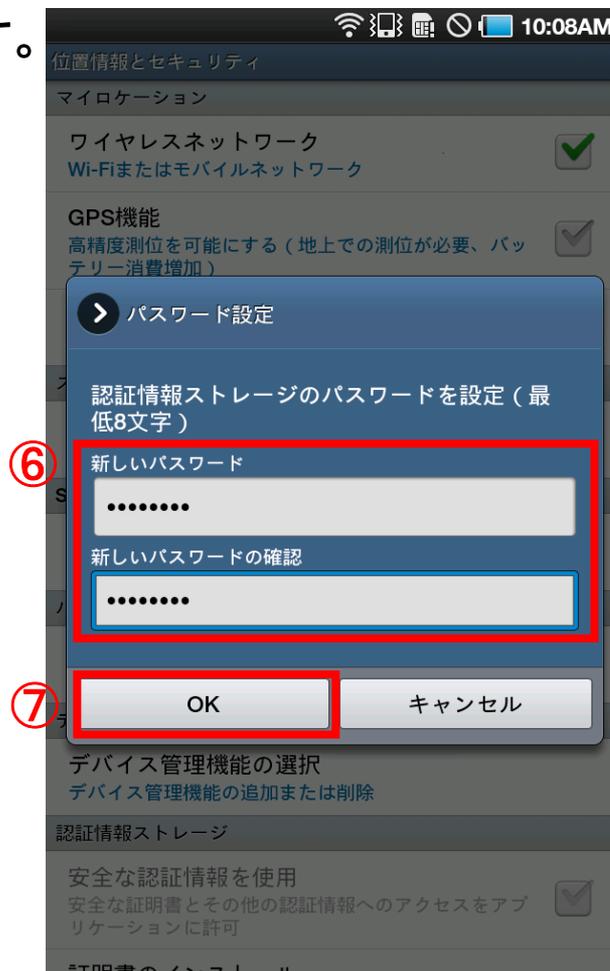


【EAP-TLSの設定方法】

STEP2. クライアント証明書を端末にインストールします。

⑥認証情報ストレージのパスワード設定を要求されますので、設定します。

⑦「OK」をタップします。



以上で、端末へのインストールは完了です。

【EAP-TLSの設定方法】

STEP3.ネットワークの設定をします。

①「無線とネットワーク」をタップします。

②「Wi-Fi設定」をタップします。



【EAP-TLSの設定方法】

STEP3.ネットワークの設定をします。

③「Wi-Fi」をタップしてWi-Fi機能をONにします。

④「Wi-Fiネットワーク」一覧の一番下にある項目「Wi-Fiネットワークを追加」をタップします。



【EAP-TLSの設定方法】

STEP3.ネットワークの設定をします。

⑤「ネットワークSSID」にESSIDを入力します。

⑥「セキュリティ設定」をタップして、「802.1x EAP」を選択します。

※ESSID,暗号方式はそれぞれのネットワークにより異なります。ご使用の環境に合わせて設定してください。



【EAP-TLSの設定方法】

STEP3.ネットワークの設定をします。

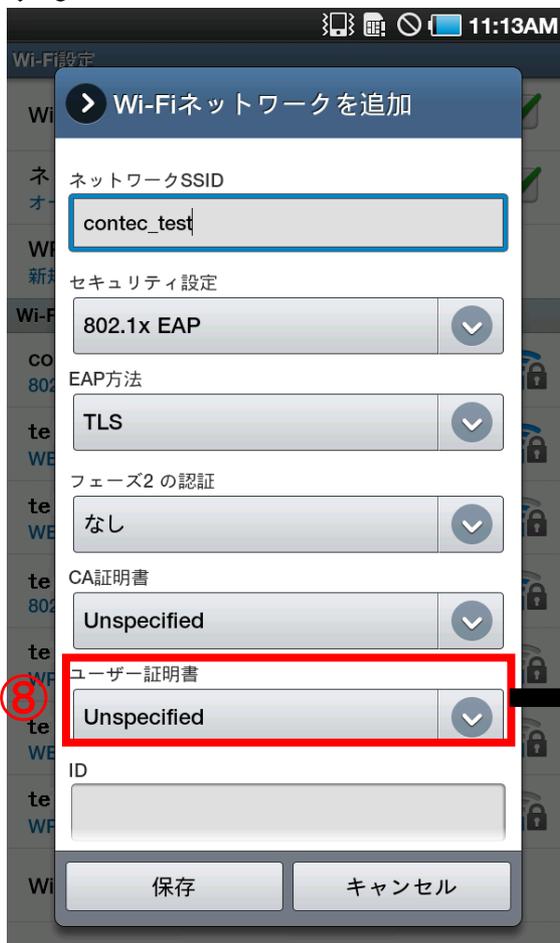
⑦「EAP方法」をタップして、「TLS」を選択します。



【EAP-TLSの設定方法】

STEP3.ネットワークの設定をします。

⑧「ユーザ証明書」をタップして、SDカードからインストールしたクライアント証明書を選択します。



【EAP-TLSの設定方法】

STEP3.ネットワークの設定をします。

⑨「ID」にユーザ名、「パスワード」にパスワードを入力して「保存」をタップします。

⑩右図のように「接続しました」と表示が出れば接続成功です。

⑨「ID」にユーザ名、「パスワード」にパスワードを入力して「保存」をタップします。

⑩右図のように「接続しました」と表示が出れば接続成功です。

「ID」「パスワード」にはSTEP1.⑪で設定した「アカウント」と「パスワード」を入力

⑩

以上で、設定は完了です。

4. PEAPの設定方法

※スマートフォンIS03は、PEAP認証時の設定方法が他端末と異なる為、P.51「5.証明書を必要とする場合のPEAPの設定方法」をご覧ください。

【PEAPの設定方法】

PEAP認証を行う場合、RADIUSサーバの設定を行う必要があります。
なお、証明書をAndroid端末にインストールする必要はありません。

下記 STEP1～2 の手順で設定方法を説明します。

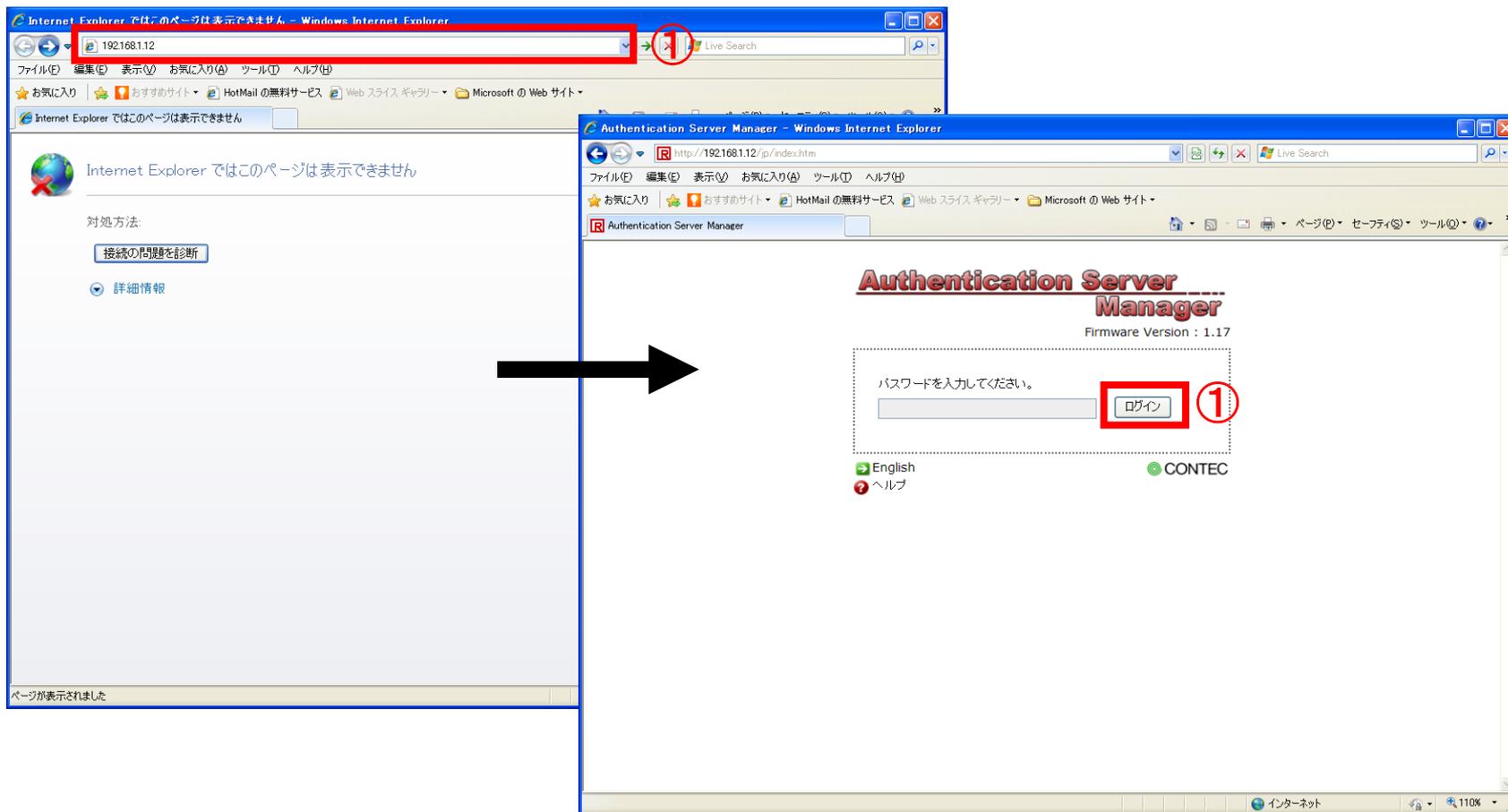
- ・STEP1.RADIUSサーバを設定
- ・STEP2.ネットワーク設定

※スマートフォンIS03は、クライアント証明書をインストールする必要がありますので、
P.51「5.クライアント証明書を必要とする場合のPEAPの設定方法」をご覧ください。

【PEAPの設定方法】

STEP1. RADIUSサーバを設定します。

①ブラウザのアドレスバーにFX-SVR-RDSのIPアドレスを入力して、機器にログインします。



【PEAPの設定方法】

STEP1. RADIUSサーバを設定します。

②「トップ」→「設定」→「基本設定」の順にクリックします。

③基本設定画面で、各項目を入力して、「確定」をクリックします。

The screenshot shows the 'Authentication Server Manager' web interface. The browser address bar shows 'http://192.168.1.12/jp/top.htm'. The page title is 'Authentication Server Manager'. The main content area is titled '設定' (Settings) and '基本設定' (Basic Settings). The configuration table is as follows:

ホスト名(必須)	host
言語設定	日本語
パスワード
パスワード(確認用)
IPアドレス	192 . 168 . 1 . 12
サブネットマスク	255 . 255 . 255 . 0
デフォルトゲートウェイ	0 . 0 . 0 . 0
DNSサーバ	0 . 0 . 0 . 0
VLAN	VLAN 機能: 無効
	VLAN ID: 0
	設定ファイル暗号化: 無効

At the bottom of the configuration area, there are two buttons: '確定' (Confirm) and 'リセット' (Reset). The '確定' button is highlighted with a red box.

【PEAPの設定方法】

STEP1. RADIUSサーバを設定します。

④「認証局」→「認証局情報」の順にクリックします。

⑤認証局情報画面で、
各項目を入力して、「作成」
をクリックします。

Authentication Server Manager - Windows Internet Explorer

http://192.168.1.12/jp/top.htm

Authentication Server Manager

CONTEC ver. 1.17

FX-SVR-RDS Authentication Server Manager

設定

認証局情報

ここで確定させた情報を元にサーバ証明書を作成します。
「作成」ボタンを押した後にサーバ証明書が自動で作成されます。

④

⑤

「有効期限」は、デフォルトで「730(日)」と入力されていますが、
変更することも可能です。

⑤

作成 クリア

ページが表示されました

【PEAPの設定方法】

STEP1. RADIUSサーバを設定します。

⑥「オーセンティケータ」をクリックします。

⑦オーセンティケータ画面

で、各項目を入力して、

「追加」をクリックします。

Authentication Server Manager - Windows Internet Explorer

http://192.168.1.12/jp/top.htm

Authentication Server Manager

CONTEC ver. 1.17

FX-SVR-RDS Authentication Server Manager

設定

オーセンティケータ

オーセンティケータの追加

IPアドレス: 192.168.1.11

共有シークレット: concet_test

追加

クリア

「IPアドレス」には、アクセスポイントのIPアドレスを入力します。
「共有シークレット」には、アクセスポイント側でも同じ値を入力します。

【PEAPの設定方法】

STEP1. RADIUSサーバを設定します。

⑧オーセンティケーター一覧に前ページで設定したIPアドレスが追加されている事を確認します。

The screenshot shows the 'Authentication Server Manager' web interface. The main content area is titled '設定' (Settings) and contains a section for 'オーセンティケーター' (Authentication Servers). Below this, there is a form for adding a new authentication server with fields for 'IP アドレス' (IP Address) and '共有シークレット' (Shared Secret). Below the form is a table titled 'オーセンティケーター一覧' (Authentication Servers List) with the following data:

No.	IP アドレス	削除 ALL
1	192.168.1.11	<input type="checkbox"/>

A red box highlights the table, and a circled '8' is placed next to it, indicating the step to verify the IP address.

【PEAPの設定方法】

STEP1. RADIUSサーバを設定します。

⑨「ユーザ管理」をクリックします。

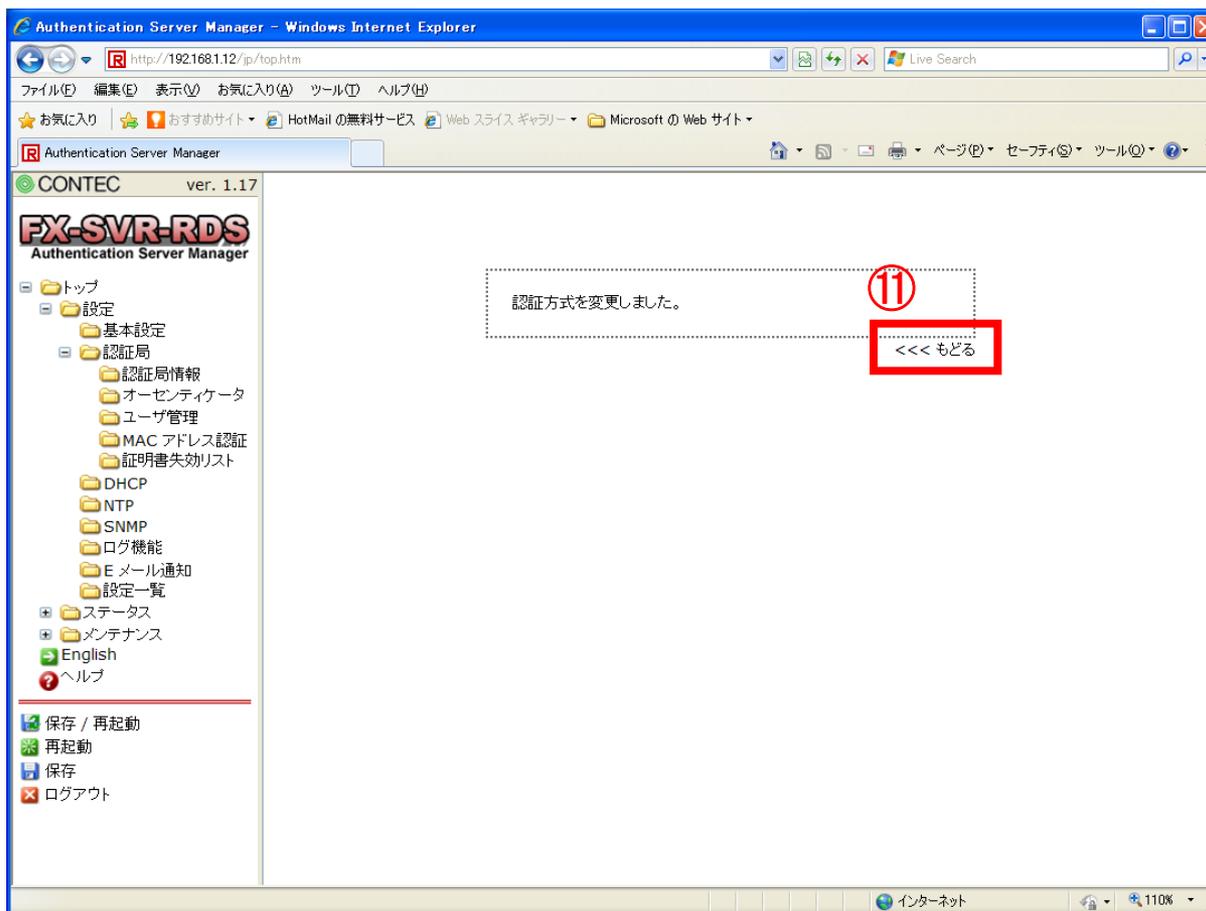
⑩「認証方式」で「PEAP」を選択し、「確定」をクリックします。

The screenshot shows the Authentication Server Manager web interface in Internet Explorer. The browser address bar shows <http://192.168.1.12/jp/top.htm>. The page title is "Authentication Server Manager ver. 1.17". The main content area is titled "設定" (Settings) and "ユーザ管理" (User Management). The "認証方式" (Authentication Method) section is highlighted with a red box and a circled "10". It shows a dropdown menu set to "PEAP", a table with "有効期限(日)" (Validity Period) set to "2013.07.24 04:03 GMT", and "ダウンロード" (Download) buttons for "DER 形式" and "PEM 形式". Below this is a "確定" (Confirm) button, also highlighted with a red box and a circled "10". The left sidebar shows a tree view with "ユーザ管理" (User Management) highlighted with a red box and a circled "9". Below the "ユーザ管理" section, there is a "新規追加" (New Addition) section with input fields for "アカウント" (Account), "パスワード" (Password), and "パスワード(確認用)" (Password (Confirmation)), and "追加" (Add) and "クリア" (Clear) buttons.

【PEAPの設定方法】

STEP1. RADIUSサーバを設定します。

⑪「認証方式を変更しました。」という表示が出ますので、「<<<もどる」をクリックします。



【PEAPの設定方法】

STEP1. RADIUSサーバを設定します。

⑫「ユーザ管理」で「アカウント」と「パスワード」を入力して、「追加」をクリックします。

Authentication Server Manager - Windows Internet Explorer

http://192.168.1.12/jp/top.htm

Authentication Server Manager ver. 1.17

FX-SVR-RDS Authentication Server Manager

設定

ユーザ管理

認証方式

認証方式	PEAP
有効期限(日)	2013.07.24 04:03 G
ダウンロード	DER 形式 PEM 形

確定 クリア

ユーザ管理

新規追加

アカウント	contec_user
パスワード
パスワード(確認用)

⑫ 追加 クリア

「アカウント」と「パスワード」は、端末でネットワーク接続の設定をする際、入力を求められます。

【PEAPの設定方法】

STEP1. RADIUSサーバを設定します。

⑬前ページで追加したアカウントが、「アカウント一覧」に追加されている事を確認して、「保存/再起動」をクリックします。

The screenshot shows the Authentication Server Manager web interface in Internet Explorer. The left sidebar contains a navigation menu with items like '設定' (Settings), 'ステータス' (Status), and 'ヘルプ' (Help). The main content area is divided into sections: '認証方式' (Authentication Method) set to 'PEAP', 'サーバ証明書' (Server Certificate) with expiration date '2013.07.24 04:03 GMT', and 'ユーザ管理' (User Management). Under 'ユーザ管理', there is a '新規追加' (New Addition) form with fields for 'アカウント' (Account), 'パスワード' (Password), and 'パスワード(確認用)' (Password Confirmation). Below this is the 'アカウント一覧' (Account List) table, which is highlighted with a red box. The table has columns for 'No.', 'アカウント', 'フィルタ ID', '設定変更', and '削除'. A single account 'contec_user' is listed. A red box also highlights the '保存 / 再起動' (Save / Restart) button in the sidebar, with a circled '13' next to it. Another circled '13' is next to the table. A pink callout box at the bottom right states: '以上で、RADIUSサーバの設定は完了です。' (With this, the RADIUS server configuration is complete.)

Authentication Server Manager - Windows Internet Explorer

http://192.168.1.12/jp/top.htm

Authentication Server Manager ver. 1.17

FX-SVR-RDS Authentication Server Manager

認証方式: PEAP

サーバ証明書: 有効期限(日) 2013.07.24 04:03 GMT

ダウンロード: DER 形式, PEM 形式

ユーザ管理

新規追加

No.	アカウント	フィルタ ID	設定変更	削除
1	contec_user		設定変更	ALL

保存 / 再起動

アカウント一覧

以上で、RADIUSサーバの設定は完了です。

【PEAPの設定方法】

①「無線とネットワーク」をタップします。

②「Wi-Fi設定」をタップします。

①



②



【PEAPの設定方法】

- ③「Wi-Fi」をタップしてWi-Fi機能をONにします。
- ④「Wi-Fiネットワークを追加」をタップします。
- ⑤「ネットワークSSID」にESSIDを入力します。

※ESSID,暗号方式はそれぞれのネットワークにより異なります。ご使用の環境に合わせて設定してください。



【PEAPの設定方法】

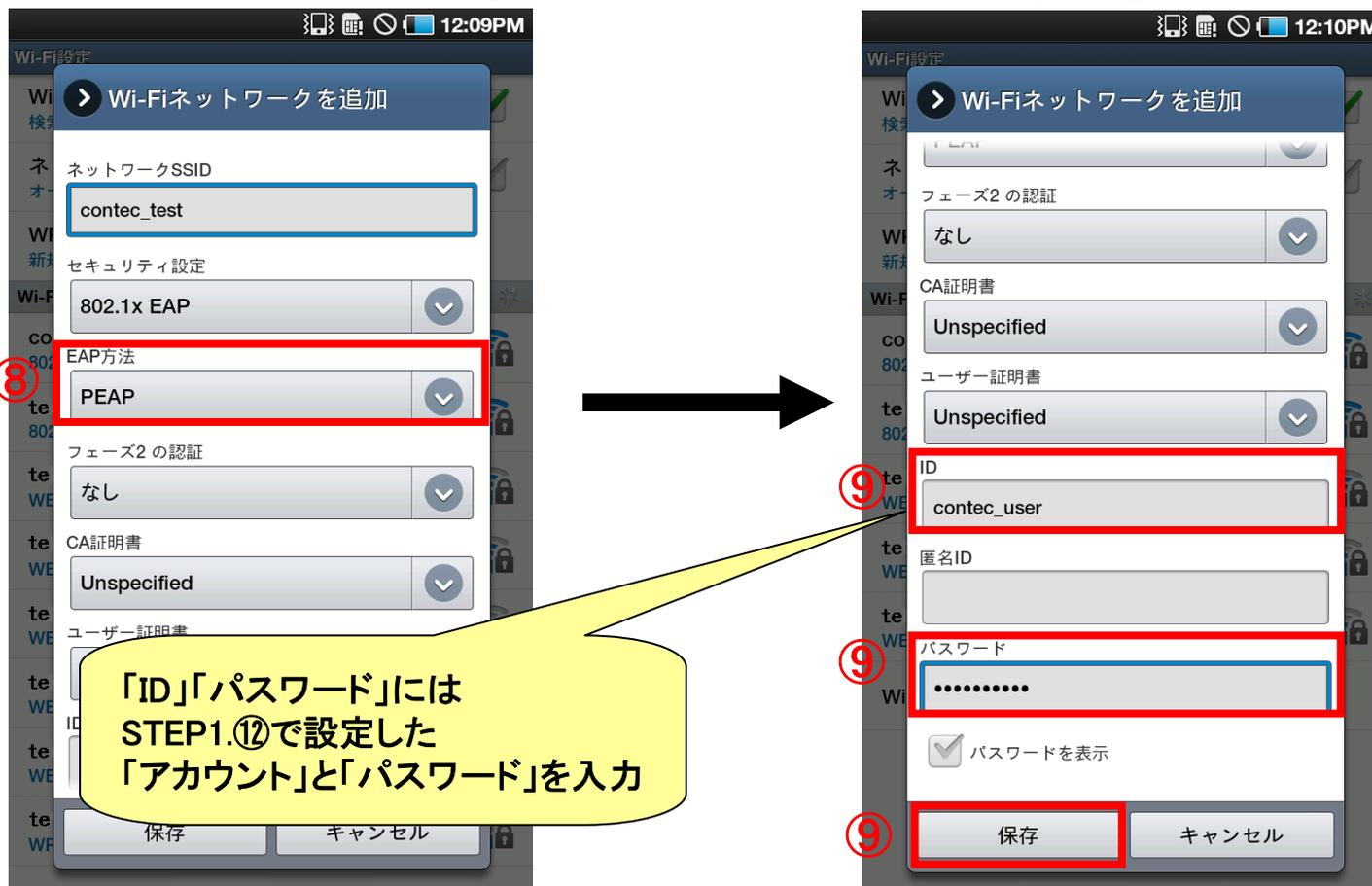
⑥「セキュリティ設定」をタップします。

⑦「802.1x EAP」を選択します。



【PEAPの設定方法】

- ⑧「EAP方法」が「PEAP」である事を確認します。「PEAP」でなければ、タップして「PEAP」を選択します。
- ⑨「ID」にユーザ名、「パスワード」にパスワードを入力して、「保存」をタップします。



【PEAPの設定方法】

⑩下図のように「接続しました」と表示が出れば接続成功です。



以上で、設定は完了です。

5. クライアント証明書が必要とする場合の PEAPの設定方法

※スマートフォンIS03は、PEAP認証時の設定方法が他機種と異なる為、この章で設定方法を説明します。

【PEAPの設定方法】

スマートフォンIS03 でPEAP認証を行う場合、RADIUSサーバの設定を行い、クライアント証明書をダウンロード後、証明書を端末へインストールする必要があります。

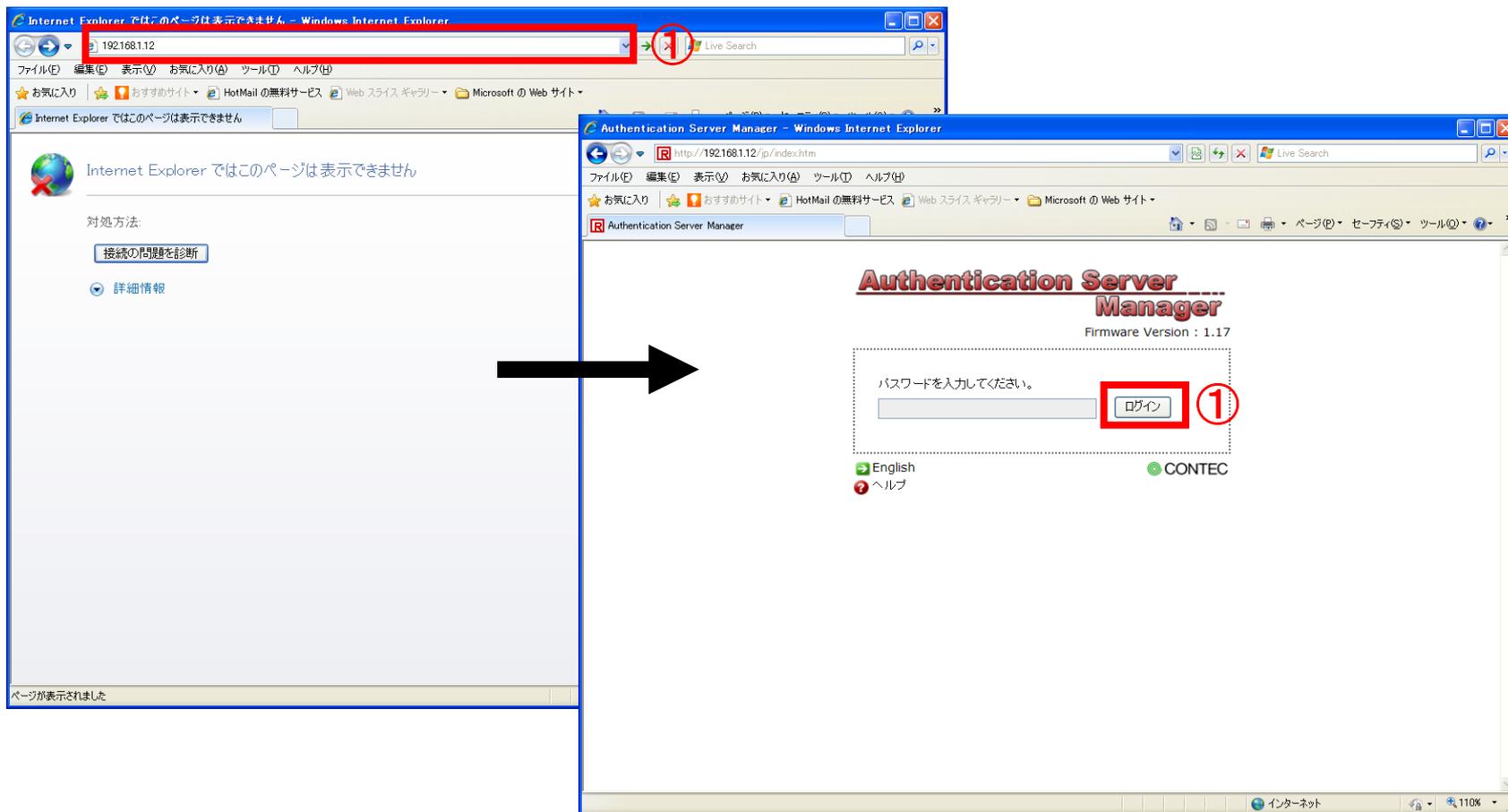
下記 STEP1～3 の手順で設定方法を説明します。

- ・STEP1.クライアント証明書の作成
- ・STEP2.クライアント証明書を端末にインストール
- ・STEP3.ネットワーク設定

【PEAPの設定方法】

STEP1. クライアント証明書を作成します。

①ブラウザのアドレスバーにFX-SVR-RDSのIPアドレスを入力して、機器にログインします。



【PEAPの設定方法】

STEP1. クライアント証明書を作成します。

②「トップ」→「設定」→「基本設定」の順にクリックします。

③基本設定画面で、各項目を入力して、「確定」をクリックします。

The screenshot shows the 'Authentication Server Manager' web interface. The browser address bar shows 'http://192.168.1.12/jp/top.htm'. The page title is 'Authentication Server Manager'. The left sidebar contains a navigation menu with the following items: 'トップ', '設定', '基本設定', '認証局', 'DHCP', 'NTP', 'SNMP', 'ログ機能', 'Eメール通知', '設定一覧', 'ステータス', 'メンテナンス', 'English', and 'ヘルプ'. The '設定' and '基本設定' items are highlighted with a red box and a circled '2'. The main content area shows the '基本設定' page with a large red 'X' and '設定' text. The form contains the following fields:

ホスト名(必須)	host
言語設定	日本語
パスワード
パスワード(確認用)
IPアドレス	192 .168 .1 .12
サブネットマスク	255 .255 .255 .0
デフォルトゲートウェイ	0 .0 .0 .0
DNSサーバー	0 .0 .0 .0
VLAN	VLAN 機能: 無効
	VLAN ID: 0
	設定ファイル暗号化: 無効

At the bottom of the form, there are two buttons: '確定' (Confirm) and 'リセット' (Reset). The '確定' button is highlighted with a red box and a circled '3'.

【PEAPの設定方法】

STEP1. クライアント証明書を作成します。

④「認証局」→「認証局情報」の順にクリックします。

⑤認証局情報画面で、
各項目を入力して、「作成」
をクリックします。

④

⑤

「有効期限」は、デフォルトで「730(日)」と入力されていますが、
変更することも可能です。

⑤

【PEAPの設定方法】

STEP1. クライアント証明書を作成します。

⑥「オーセンティケータ」をクリックします。

⑦オーセンティケータ画面
で、各項目を入力して、
「追加」をクリックします。

「IPアドレス」には、アクセスポイントのIPアドレスを入力します。
「共有シークレット」には、アクセスポイント側でも同じ値を入力します。

【PEAPの設定方法】

STEP1. クライアント証明書を作成します。

⑧オーセンティケーター一覧に前ページで設定したIPアドレスが追加されている事を確認します。

The screenshot shows the 'Authentication Server Manager' web interface in Internet Explorer. The main content area is titled '設定' (Settings) and 'オーセンティケーター' (Authenticator). Below this, there is a section for adding authenticators and a table listing existing ones.

オーセンティケーター追加

IP アドレス: [.] [.] [.] [.]
 共有シークレット: []

[追加] [クリア]

オーセンティケーター一覧

No.	IP アドレス	削除 ALL
1	192.168.1.11	<input type="checkbox"/>

[削除] [クリア]

A red box highlights the table, and a circled '8' is placed next to it, indicating the step to verify the IP address.

【PEAPの設定方法】

STEP1. クライアント証明書を作成します。

⑨「ユーザ管理」をクリックします。

⑩「認証方式」で「EAP-TLS」を選択して、「確定」をクリックします。

The screenshot shows the Authentication Server Manager web interface in Internet Explorer. The browser address bar shows <http://192.168.1.12/jp/top.htm>. The page title is "Authentication Server Manager ver. 1.17". The main content area is titled "設定" (Settings) and "ユーザ管理" (User Management). The "認証方式" (Authentication Method) section is highlighted with a red box and a circled "10". The "認証方式" dropdown menu is set to "EAP-TLS". Below this, the "サーバ証明書" (Server Certificate) section shows the expiration date as "2015-07-24 04:03 GMT" and the download button as "DER 形式". The "確定" (Confirm) button is also highlighted with a red box and a circled "10". The left sidebar shows the "ユーザ管理" (User Management) menu item highlighted with a red box and a circled "9". A yellow callout box points to the "EAP-TLS" selection with the text: "認証方式を「PEAP」に設定すると、クライアント証明書をダウンロードできない為、「EAP-TLS」に設定します。"

認証方式	
認証方式	EAP-TLS
サーバ証明書	有効期限(日) 2015-07-24 04:03 GMT ダウンロード DER 形式

ユーザ管理	
新規追加	
アカウント	
パスワード	
パスワード(確認用)	

【PEAPの設定方法】

STEP1. クライアント証明書を作成します。

⑪「ユーザ管理」で「アカウント」と「パスワード」を入力して、「追加」をクリックします。

The screenshot shows the 'Authentication Server Manager' web interface. The left sidebar contains a navigation menu with items like 'トップ', '設定', '認証局', 'DHCP', 'NTP', 'SNMP', 'ログ機能', 'Eメール通知', '設定一覧', 'ステータス', 'メンテナンス', 'English', and 'ヘルプ'. The main content area is titled '設定' (Settings) and 'ユーザ管理' (User Management). Under 'ユーザ管理', there is a '新規追加' (New Addition) section. This section contains a form with three input fields: 'アカウント' (Account) with the value 'contec_user', 'パスワード' (Password) with masked characters, and 'パスワード(確認用)' (Password (Confirmation)). Below the form are '追加' (Add) and 'クリア' (Clear) buttons. A red box highlights the entire '新規追加' form area, and a red circle with the number '11' is placed over the '追加' button. A yellow callout bubble with a black border contains the text: 「アカウント」と「パスワード」は、端末でネットワーク接続の設定をする際、入力を求められます。 (Account and Password are required for network connection settings on the terminal.)

【PEAPの設定方法】

STEP1. クライアント証明書を作成します。

⑫前ページで追加したアカウントが、「アカウント一覧」に追加されている事を確認して、「発行/変更」をクリックします。

The screenshot shows the Authentication Server Manager web interface. The left sidebar contains a navigation menu with options like '設定' (Settings), 'ステータス' (Status), and 'ヘルプ' (Help). The main content area is divided into sections: 'サーバ証明書' (Server Certificate), 'ユーザ管理' (User Management), and 'アカウント一覧' (Account List). The 'アカウント一覧' section shows a table of accounts with a red box highlighting the first row and the '発行/変更' button. A circled '12' is placed over the button.

No.	アカウント	フィルタ ID	ステータス / 有効期限	クライアント証明書 / 設定変更	削除
1	contec_user		未発行	発行/変更	<input type="checkbox"/>

【PEAPの設定方法】

STEP1. クライアント証明書を作成します。

⑬左下のウィンドウで、「有効期限(日)」を入力して「設定変更」をクリックします。

⑭「証明書出力形式」で「PKCS#12(ルート証明書含む)」を選択し、「発行」をクリックします。

デフォルトで「365」と入力されていますが、有効期限を変更する事ができます。

項目	値
アカウント	contec_user
有効期限(日)	365
フィルタ ID	
許可 MAC アドレス	00-00-00-00-00-00
許可 ESSID	
許可オーセンティケータ 1	0 . 0 . 0 . 0
許可オーセンティケータ 2	0 . 0 . 0 . 0
許可オーセンティケータ 3	0 . 0 . 0 . 0

証明書出力形式選択

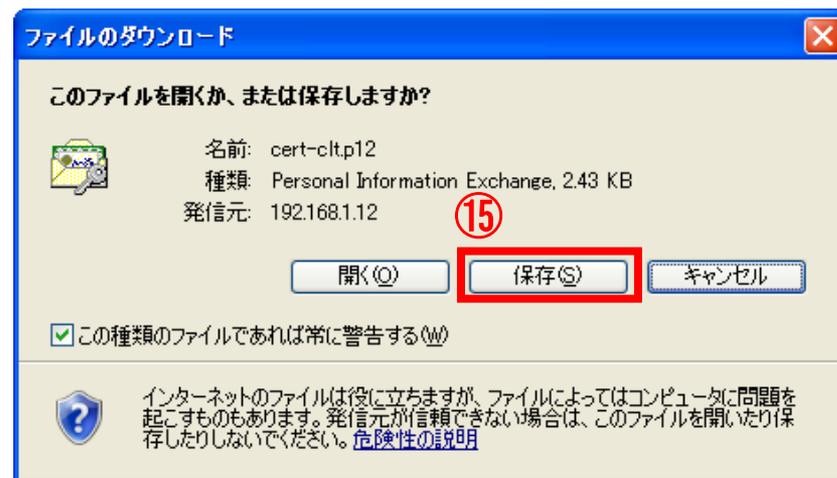
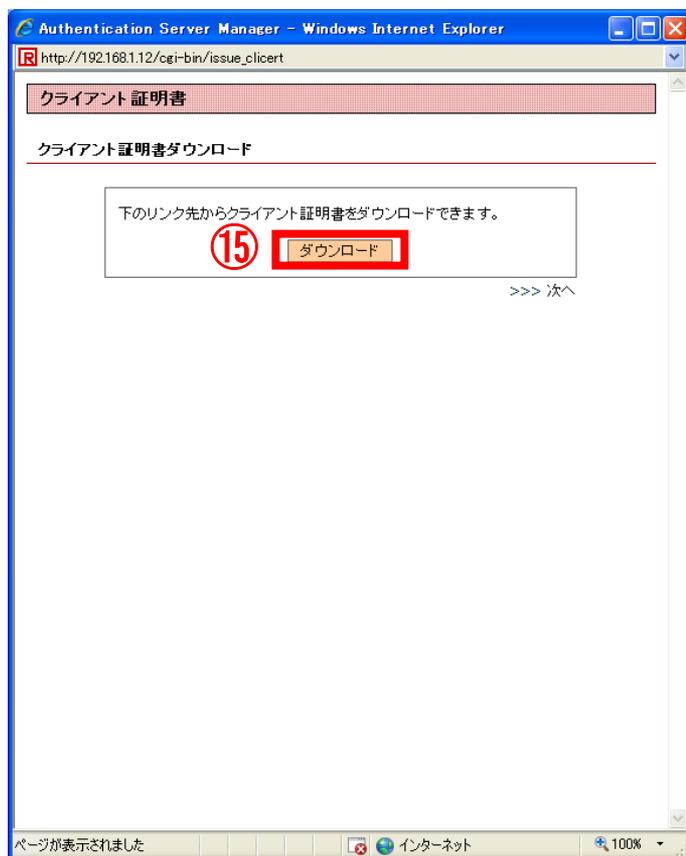
- PKCS#12 形式(ルート証明書含む)
- PKCS#12 形式(ルート証明書含まない)
- DER 形式(秘密鍵暗号化有)
- DER 形式(秘密鍵暗号化無)
- PEM 形式(秘密鍵暗号化有)
- PEM 形式(秘密鍵暗号化無)

ファイル暗号化パスワード:

【PEAPの設定方法】

STEP1. クライアント証明書を作成します。

⑮ 「ダウンロード」をクリック後、「保存」で、クライアント証明書をダウンロードします。



【PEAPの設定方法】

STEP1. クライアント証明書を作成します。

⑩「認証方式」を「PEAP」に選択しなおして、「確定」をクリックします。

⑪「保存/再起動」をクリックして、再起動します。

The screenshot shows the 'Authentication Server Manager' web interface in Internet Explorer. The browser address bar shows 'http://192.168.1.12/jp/top.htm'. The page title is 'Authentication Server Manager'. The interface is in Japanese and shows the 'FX-SVR-RDS Authentication Server Manager' configuration page. The '認証方式' (Authentication Method) dropdown menu is set to 'PEAP', highlighted with a red box and a circled '16'. Below it, the 'サーバ証明書' (Server Certificate) section shows '有効期限(日)' (Validity Period) as '2013.07.24 04:03 GMT' and 'ダウンロード' (Download) buttons for 'DER形式' and 'PEM形式'. A '確定' (Confirm) button is also highlighted with a red box and a circled '16'. The 'ユーザ管理' (User Management) section has a '新規追加' (New Add) button. Below it, there are input fields for 'アカウント' (Account), 'パスワード', and 'パスワード(確認用)' (Password Confirmation), with '追加' and 'クリア' buttons. The 'アカウント一覧' (Account List) section shows a table with one account: 'contec_user' with status '2012.07.24 04:08 GMT' and a '発行/変更' (Issue/Change) button. A '保存 / 再起動' (Save / Restart) button is highlighted with a red box and a circled '17' in the bottom left corner of the interface.

以上で、クライアント証明書の作成は完了です。

【PEAPの設定方法】

STEP2. クライアント証明書を端末にインストールします。

端末にクライアント証明書をインストールするには、microSDカードが必要です。microSDカードにSTEP1.⑮でダウンロードしたクライアント証明書を保存して、端末に挿入してください。

【PEAPの設定方法】

STEP2. クライアント証明書を端末にインストールします。

①「現在地情報とセキュリティ」をタップします。

②「証明書のインストール」をタップします。

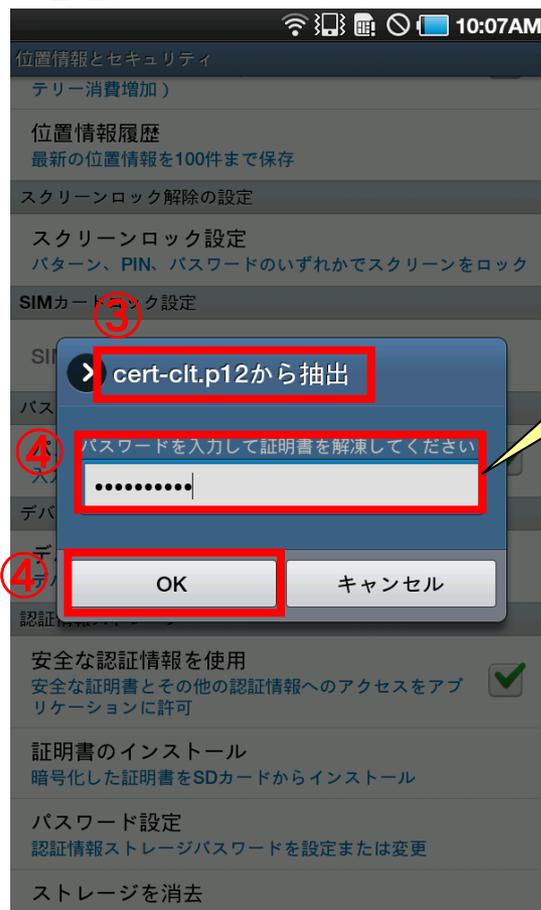


【PEAPの設定方法】

STEP2. クライアント証明書を端末にインストールします。

③SDカード内にあるクライアント証明書ファイル名が表示されます。

④パスワードを入力して、「OK」をタップします。



STEP1.⑪で設定した
パスワードを入力

【PEAPの設定方法】

STEP2. クライアント証明書を端末にインストールします。

⑤ 証明書名のウィンドウが表示されます。既に証明書名が入力されているので、そのまま「OK」をタップしても問題ありませんが、ここでは「contec_wlan」として設定します。

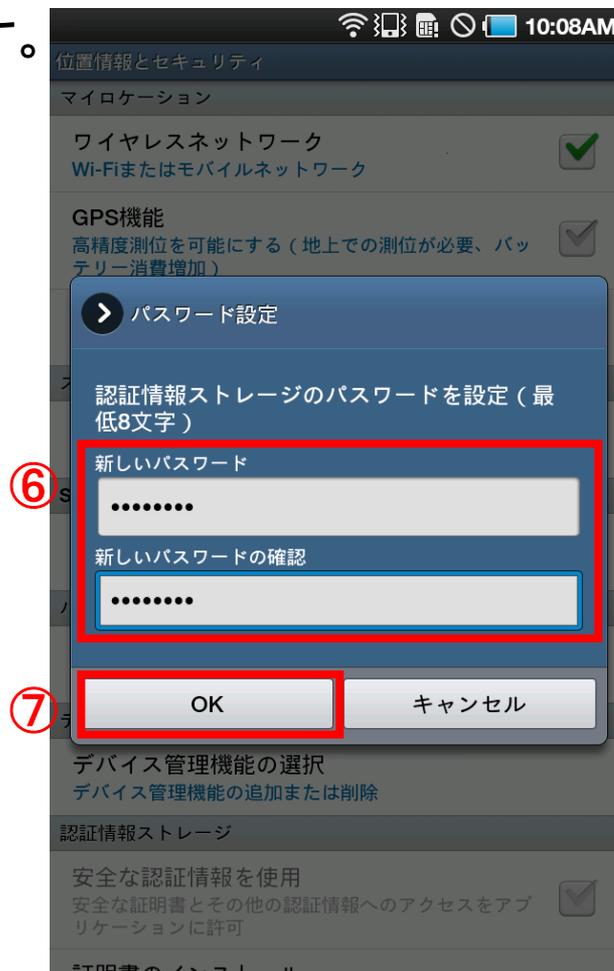


【PEAPの設定方法】

STEP2. クライアント証明書を端末にインストールします。

⑥認証情報ストレージのパスワード設定を要求されますので、設定します。

⑦「OK」をタップします。



以上で、端末へのインストールは完了です。

【PEAPの設定方法】

STEP3. ネットワークの設定をします。

①「無線とネットワーク」をタップします。

②「Wi-Fi設定」を
タップします。



【PEAPの設定方法】

STEP3. ネットワークの設定をします。

③「Wi-Fi」をタップしてWi-Fi機能をONにします。

④「Wi-Fiネットワークを追加」をタップします。

⑤「ネットワークSSID」に
ESSIDを入力します。

※ESSID,暗号方式はそれぞれのネットワークにより異なります。ご使用の環境に合わせて設定してください。



【PEAPの設定方法】

STEP3. ネットワークの設定をします。

⑥「セキュリティ設定」をタップします。

⑦「802.1x EAP」を選択
します。



【PEAPの設定方法】

STEP3. ネットワークの設定をします。

⑧「EAP方法」が「PEAP」である事を確認します。「PEAP」でなければ、「PEAP」を設定します。

⑨「CA証明書」を選択して、「ID」にユーザ名、「パスワード」にパスワードを入力して、「保存」をタップします。



「ユーザ証明書」ではなく「CA証明書」で、インストールした証明書を選択してください。

「ID」「パスワード」にはSTEP1.⑪で設定した「アカウント」と「パスワード」を入力

【PEAPの設定方法】

STEP3. ネットワークの設定をします。

⑩下図のように「接続しました」と表示が出れば接続成功です。



以上で、設定は完了です。